# On subsets of $GF(q^2)$ with square differences

by A. Blokhuis

*Department of Mathematics, Eindhoven University of Technology, Eindhoven, the Netherlands*

*During the period of this research the author was working at the Centre for Mathematics and Computer Science, Amsterdam, the Netherlands*

Communicated by Prof. J.H. van Lint at the meeting of September 24, 1984

ABSTRACT

The only $q$-subsets of $GF(q^2)$ with the property that the difference of any two elements is always a square or always a non-square, are the lines of $GF(q^2)$, considered as the affine plane $AG(2,q)$.

## INTRODUCTION

In [1] van Lint and MacWilliams conjecture that the only $q$-subset $X$ of $GF(q^2)$, with the properties $0,1 \in X$ and $x-y$ is a square for all $x,y \in X$, is the set $GF(q)$. For $q$ a prime this is a consequence (due to van Lint and MacWilliams) of a theorem of Rédei, cf. [3] p. 237 Satz 24'. This case was also proved in an elementary way by Lovász and Schrijver [2]. The problem arose in an attempt to characterize the vectors of minimum weight in certain quadratic residue-codes. Throughout this note we assume $q$ odd.

THE FIELD $GF(q^2)$. Let $F = GF(q^2)$. Then $F$ can be viewed in a canonical way as a two-dimensional vector space over $GF(q)$, or, as the affine plane $AG(2,q)$. The lines of this plane are $q$-subsets of $F$ with the property that the difference of two elements is either always a square, or always a non-square, depending only on the slope of the line. Thus the lines are partitioned into two classes, $S$ and $N$ (for square and non-square type). Through each point of $AG(2,q)$ there pass $(q+1)/2$ lines of $S$ and $(q+1)/2$ lines of $N$. Hence on an arbitrary line $l$ of $S$ not passing through 0, there are $(q+1)/2$ non-squares (since the line parallel to $l$ containing the origin is also in $S$).

Let $X \subset F$ be a set of points such that all differences are squares. Call such a set *special*. Then $aX$ is also special if $a$ is a square (and "anti-special" if $a$ is a non-square), and $X+a$ is special for all $a$. We will consider special $q$-sets containing 0.

NOTATION. Let $\sigma_k(X)$ denote the $k^{\text{th}}$ elementary symmetric function of the (finite) set $X$, i.e.,

$$\prod_{x \in X} (1+xt) = \sum_{k=0}^{|X|} \sigma_k(X) t^k.$$

Furthermore, if $0 \in X$, let $X_0 := X \setminus \{0\}$.

THEOREM. Let $X$ be a special $q$-set. Then $X$ is a line in $S$.

The proof will be established in a series of lemmas. Assume $0 \in X$. (If not then a translation of $X$ will do).

Let

$$f(t) := \prod_{x \in X_0} (t-x).$$

LEMMA 1. $X$ is a line iff

$$f(t) = t^{q-1} + \prod_{x \in X_0} x.$$

PROOF. ($\Rightarrow$) A line through 0 looks like $\{ia | i \in GF(q)\}$.

($\Leftarrow$) If $f(t) = t^{q-1} + \prod x$ then $x^{q-1} = y^{q-1}$ for $x, y \in X_0$. □

Since

$$f(t) = \sum_{k=0}^{q-1} (-1)^k \sigma_k(X_0) t^{q-1-k}$$

it suffices to show that $\sigma_k(X_0) = 0$ if $0 < k < q-1$.

Let $A$ be a set of $(q+1)/2$ *non-squares* such that $a-b$ is a square for $a, b \in A$. (An example of such a set is the collection of non-squares on a line in $S$, not through the origin.) Call such a set *extra-special*.

LEMMA 2. Let $A$ be any extra-special set and $X$ a special $q$-set containing 0. Then $A \cdot X_0 = \{ax | a \in A, x \in X_0\}$ is the set of all non-squares in $F$.

PROOF. Obviously $A \cdot X_0$ contains only non-squares. Since there are $\frac{1}{2}(q^2-1)$ products $ax$ involved it remains to show that all are different. Suppose $ax = by$ (with $a, b \in A$ and $x, y \in X$). Then $(a-b)x = b(y-x)$ and $(a-b)x$ is a square while $b(y-x)$ is not, unless $y = x$, but then also $a = b$. □

Let

$$f_a(t) := \prod_{x \in X_0} (t - ax) \text{ for } a \in A.$$

LEMMA 3.

$$\prod_{a\in A} f_a(t) = t^{\frac{1}{2}(q^2-1)} + 1.$$

PROOF.

$$\prod_{a\in A} f_a(t) = \prod_{\substack{a\in A \\ x\in X_0}} (t-ax) = \prod_{\substack{n\in F \\ n=\square}} (t-n) = t^{\frac{1}{2}(q^2-1)} + 1. \qquad \square$$

LEMMA 4. $\sigma_k(X_0) = 0$ if $0 < k \leq \frac{1}{2}(q-1)$.

PROOF. Let $m \leq \frac{1}{2}(q-1)$ be the smallest positive integer with the property $\sigma_m(X) \neq 0$, if such an $m$ exists. Then

$$f_a(t) = t^{q-1} + (-1)^m a^m \sigma_m(X_0) t^{q-m-1} + \text{terms of lower degree.}$$

As a consequence:

$$\prod_{a\in A} f_a(t) = t^{\frac{1}{2}(q^2-1)} + (-1)^m \Big(\sum_{a\in A} a^m\Big)\sigma_m(X_0) t^{\frac{1}{2}(q^2-1)-m} +$$

$$+ \text{terms of lower degree.}$$

Since

$$\prod_{a\in A} f_a(t) = t^{\frac{1}{2}(q^2-1)} + 1$$

and $\sigma_m(X_0) \neq 0$ it follows that

$$\sum_{a\in A} a^m = 0 \text{ for all extra-special sets } A.$$

Let $A^{(s)} = \{a^s | a \in A\}$. Then it is easy to see that $A^{(-1)}$ and $A^{(q)}$ are extra-special if $A$ is. Hence also $A^{(-q)}$ is extra-special and we have:

$$\sum_{a\in A} a^{-qm} = 0.$$

Since $a^{\frac{1}{2}(q^2-1)} = -1$ for all $a \in A$ we finally have:

$$\sum_{a\in A} a^{\frac{1}{2}(q^2-1)-qm} = 0 \text{ for all extra-special sets } A.$$

Let $t \in GF(q^2) \setminus GF(q)$ and take $A = \{t+i \,|\, i \in GF(q), t+i = \square\}$. Then

$$0 = 2 \sum_{\substack{i\in GF(q) \\ t+i=\square}} (t+i)^{\frac{1}{2}(q^2-1)-qm} =$$

$$= \sum_{i\in GF(q)} (t+i)^{\frac{1}{2}(q^2-1)-qm} - \sum_{i\in GF(q)} (t+i)^{q^2-1-qm} =: F(t).$$

The polynomial $F(t)$ vanishes for all $t \in GF(q^2) \setminus GF(q)$ and since it has degree less than $q^2 - q$ it follows that $F(t)$ is identically zero.

Consider the coefficient of $t^{q^2-qm-q}$ in $F(t)$:

$$\binom{q^2-qm-1}{q-1} \sum_{i\in GF(q)} i^{q-1} = 0.$$

But

$$\binom{q^2-qm-1}{q-1} \equiv 1 \pmod{p} \text{ and } \sum_{i \in GF(q)} i^{q-1} = q-1 \equiv -1 \pmod{p}.$$

Here $p$ is the characteristic of $GF(q)$.

This contradiction proves Lemma 4. □

To finish the proof of the theorem observe that $X_0^{(-1)} \cup \{0\}$ is also special, and as a consequence:

$$\sigma_{q-1-m}(X_0) = \prod_{x \in X_0} x \cdot \sigma_m(X_0^{(-1)}) = 0 \text{ if } 0 < m < \tfrac{1}{2}(q-1).$$

Hence $\sigma_m(X) = 0$ for all $0 < m < q-1$, and

$$f(t) = t^{q-1} + \prod_{x \in X_0} x.$$

REFERENCES


1. Lint, J.H. van and F.J. MacWilliams – Generalized Quadratic Residue Codes, IEEE Transactions on Information Theory, IT **24**, 730–737 (1978).
2. Lovász, L. and A. Schrijver – Remarks on a theorem of Rédei, Studia Scientiarum Mathematicarum Hungarica **16**, 449–454 (1981).
3. Rédei, L. – Lückenhafte Polynome über endlichen Körpern, Birkhäuser Verlag, Basel und Stuttgart, 1970.